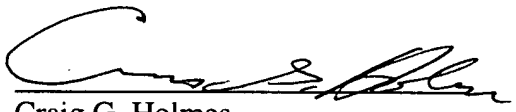
REMARKS

This Preliminary Amendment is presented to correct the references to Figures 8, 20, and 22 in the application as filed to refer to Figures 8A, 8B, 20A, 20B, 22A, and 22B, which correspond to the figure numbers of the formal drawings that were filed on December 11, 2001 in response to the Notice to File Corrected Application Papers that was mailed on October 26, 2001. No new matter is added. Entry is respectfully requested.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any fee shortages or credit any overages Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP



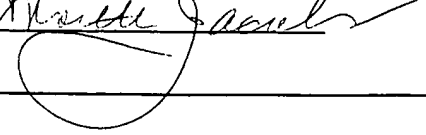
Craig G. Holmes
Reg. No. 44,770

1600 Willow Street
San Jose, CA 95125
(408) 414-1080, ext. 207
Date: February 6, 2002
Facsimile: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Hon. Commissioner for Patents, BOX NON-FEE AMEND, Washington, D.C. 20231

on February 6, 2002 by



MARKED-UP VERSION OF SPECIFICATION PARAGRAPHS

For purposes of showing the changes from the current version of the application, deleted text is shown in [brackets] and added text is underlined.

Paragraph on page 6, lines 19-20

[FIG. 8 is] FIGS. 8A-8B are a flow diagram that depicts the control flow for modular multiplication in RNS, according to an embodiment;

Paragraph on page 7, lines 17-18

[FIG. 20 is] FIGS. 20A-20B are a diagram of an array of 6 levels of 4:2 compressors, according to an embodiment;

Paragraph on page 7, line 21

[FIG. 22 is] FIGS. 22A-22B are a diagram of vector dw/v computations, according to an embodiment; and

Paragraph on page 43, lines 10-12

[FIG. 8 is] FIGS. 8A-8B are a flow diagram that depicts the control flow for modular multiplication in RNS, according to an embodiment. In [FIG. 8] FIGS. 8A-8B, rectangular blocks on the same horizontal level overlap execution times.

Paragraph on page 51, lines 22-23

[FIG. 20 is] FIGS. 20A-20B are a diagram of an array of 6 levels of 4:2 compressors organized into six levels, according to an embodiment.

Paragraph on page 52 line 3

[FIG. 22 is] FIGS. 22A-22B are a diagram of vector $d_{w/v}$ computations, according to an embodiment.